Fig 1

09/444937

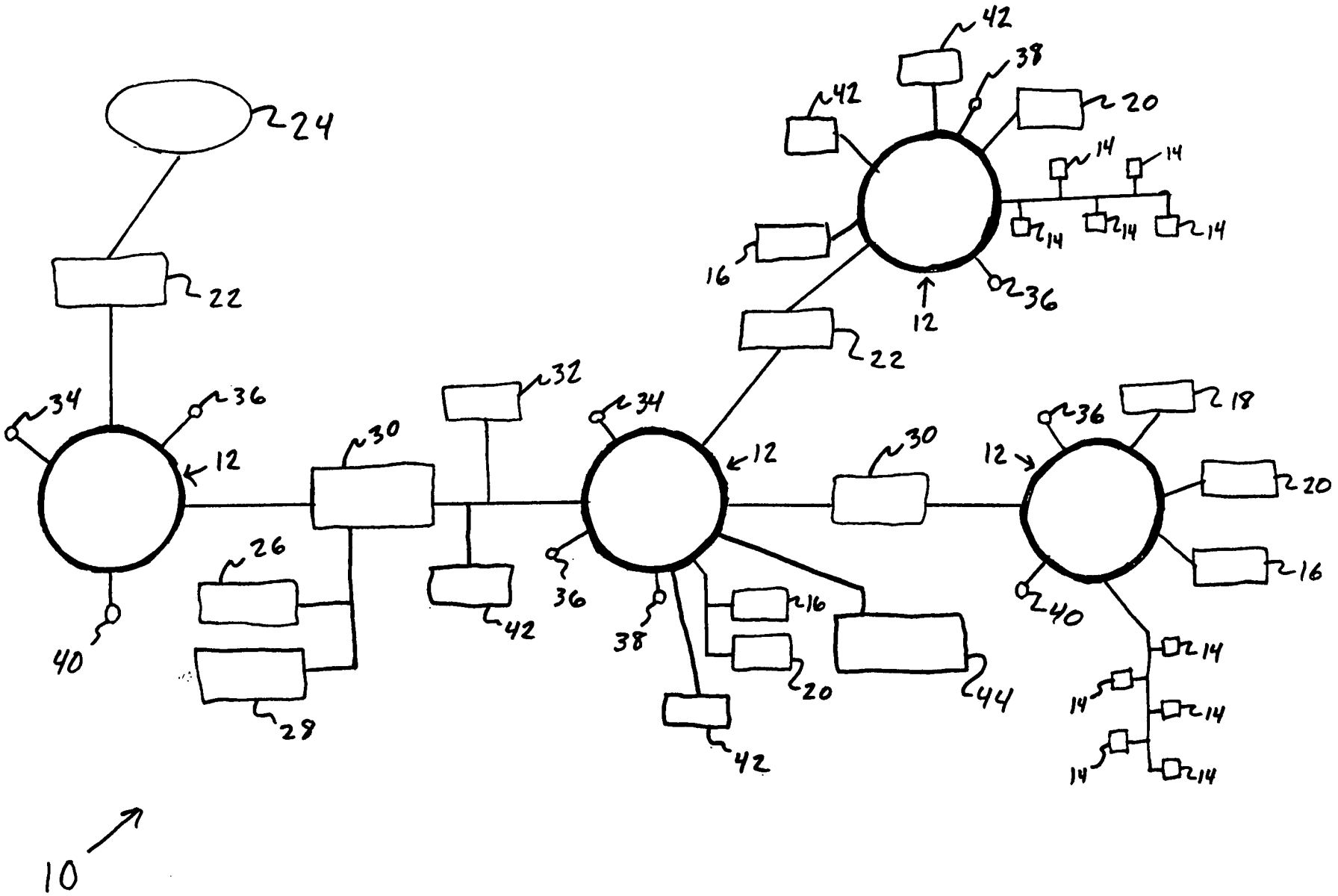


Figure 2

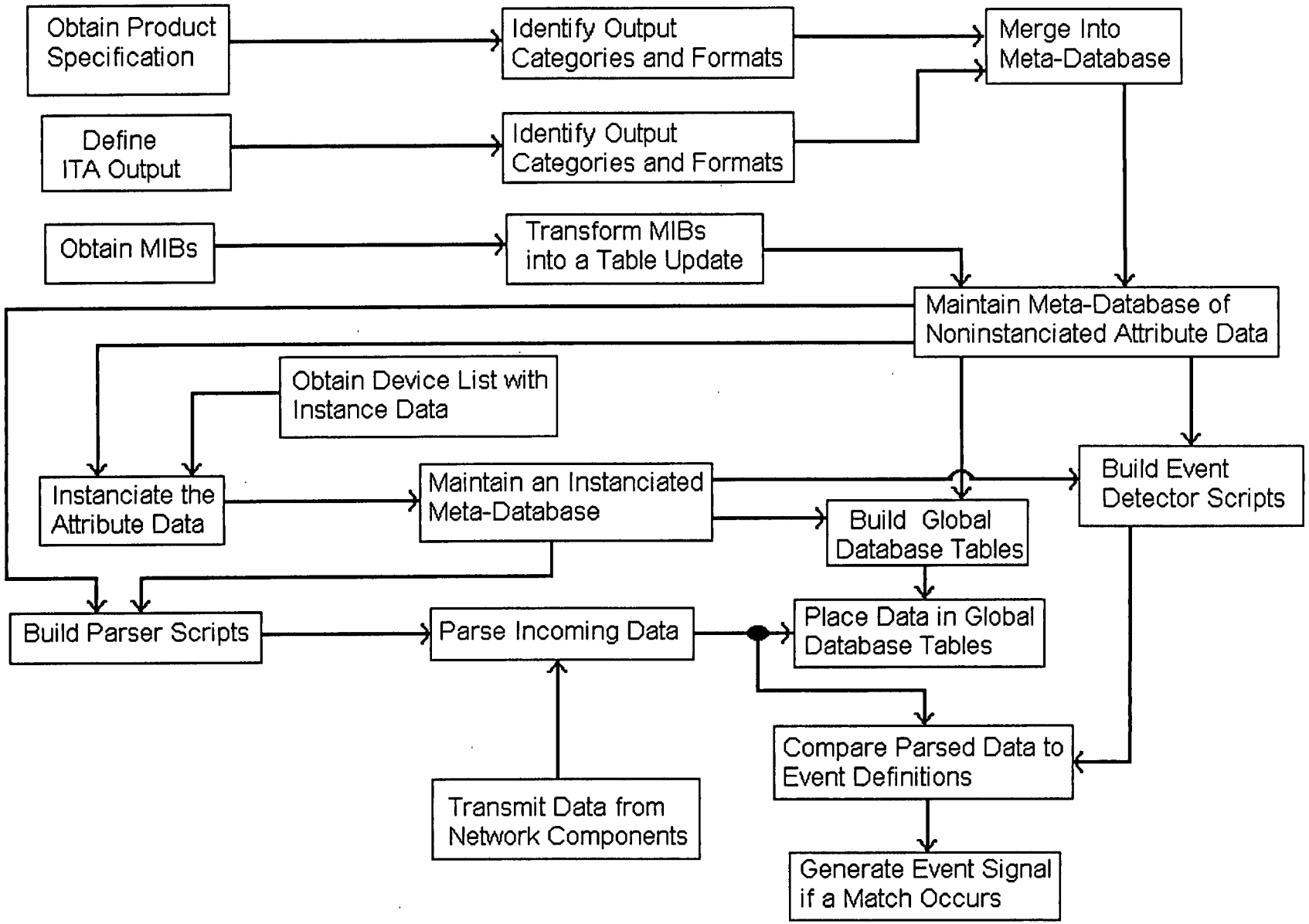
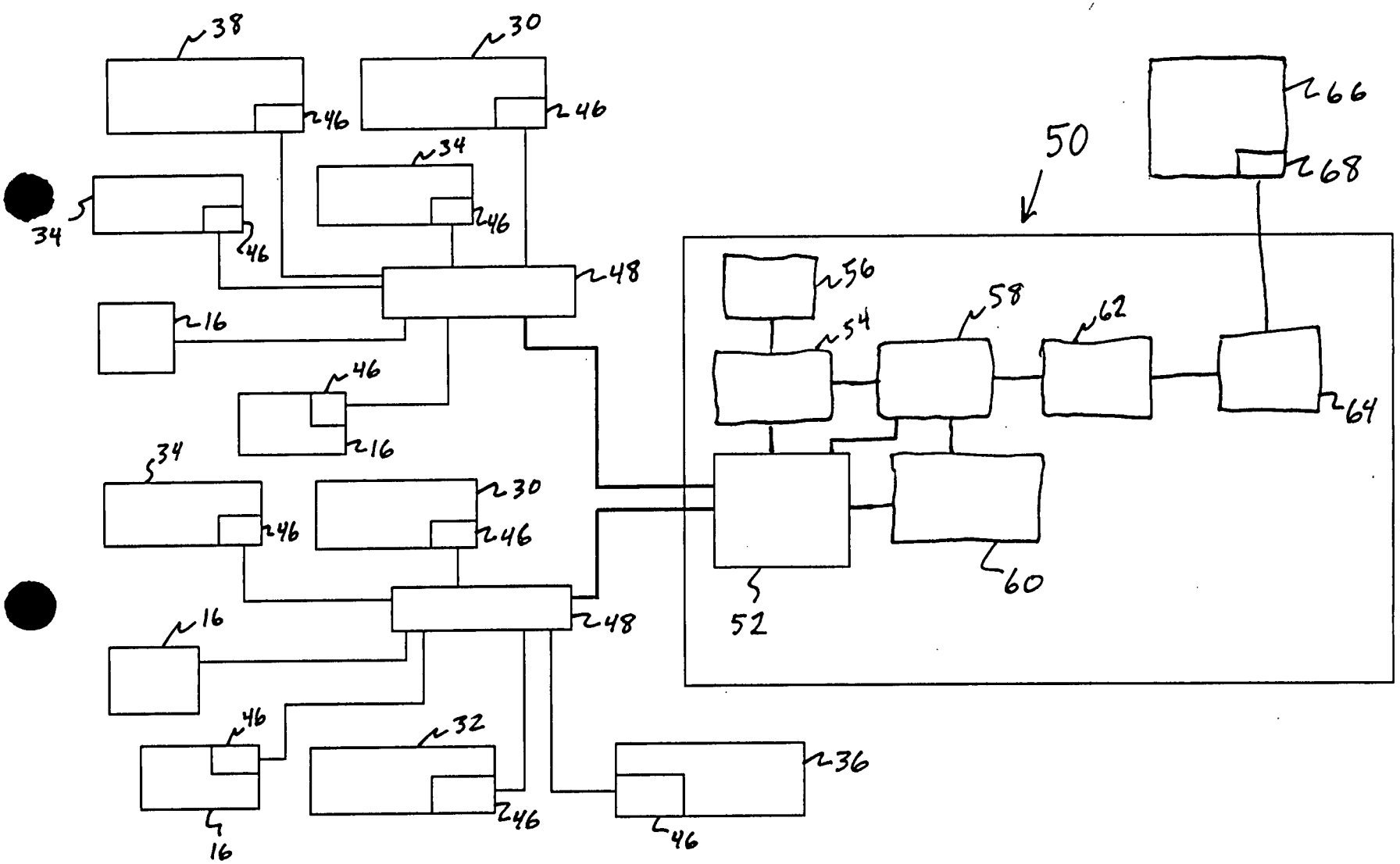

Obtain Product Specification
Identify Output Categories and Formats
Merge Into Meta-Database
Define ITA Output
Identify Output Categories and Formats
Obtain MIBs
Transform MIBs into a Table Update
Maintain Meta-Database of Noninstanciated Attribute Data
Obtain Device List with Instance Data
Instanciate the Attribute Data
Maintain an Instanciated Meta-Database
Build Event Detector Scripts
Build Global Database Tables
Build Parser Scripts
Parse Incoming Data
Place Data in Global Database Tables
Compare Parsed Data to Event Definitions
Transmit Data from Network Components
Generate Event Signal if a Match Occurs

Figure 3



09444937 .112299

Figure 4

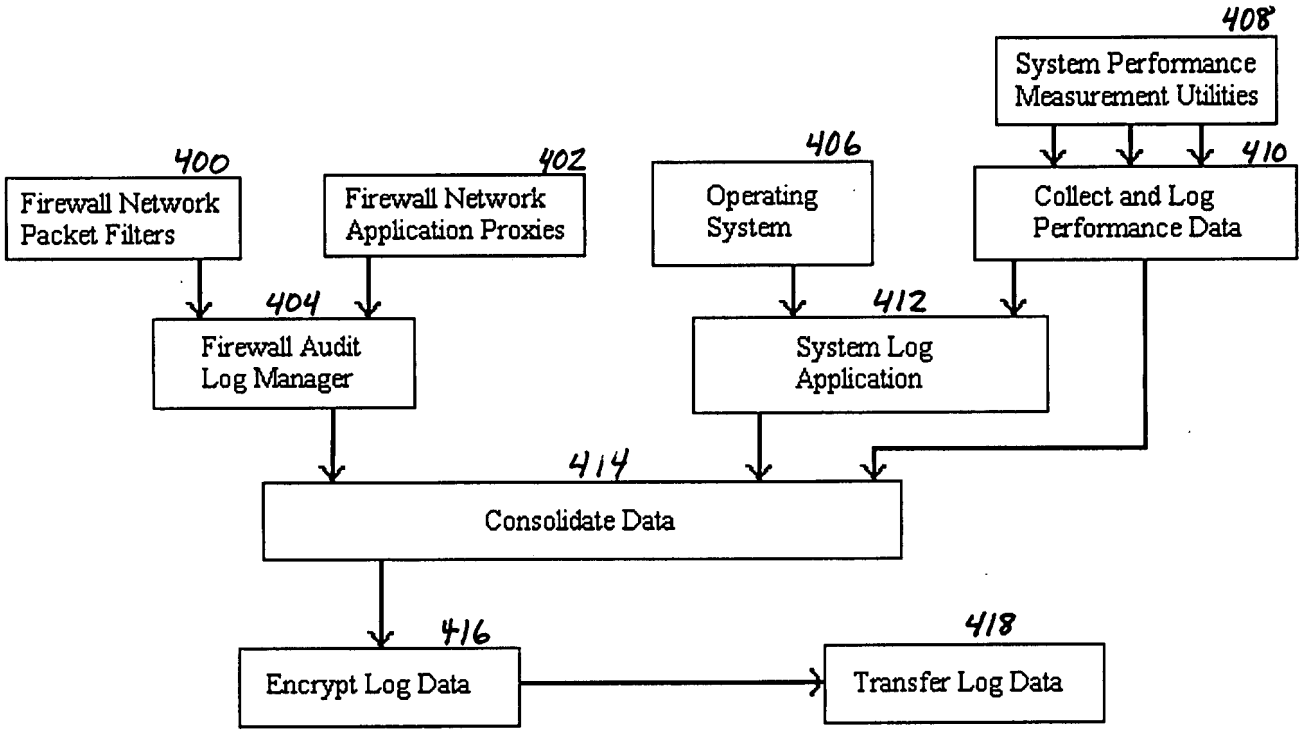

400
Firewall Network Packet Filters
402
Firewall Network Application Proxies
404
Firewall Audit Log Manager
406
Operating System
408
System Performance Measurement Utilities
410
Collect and Log Performance Data
412
System Log Application
414
Consolidate Data
416
Encrypt Log Data
418
Transfer Log Data

Figure 5

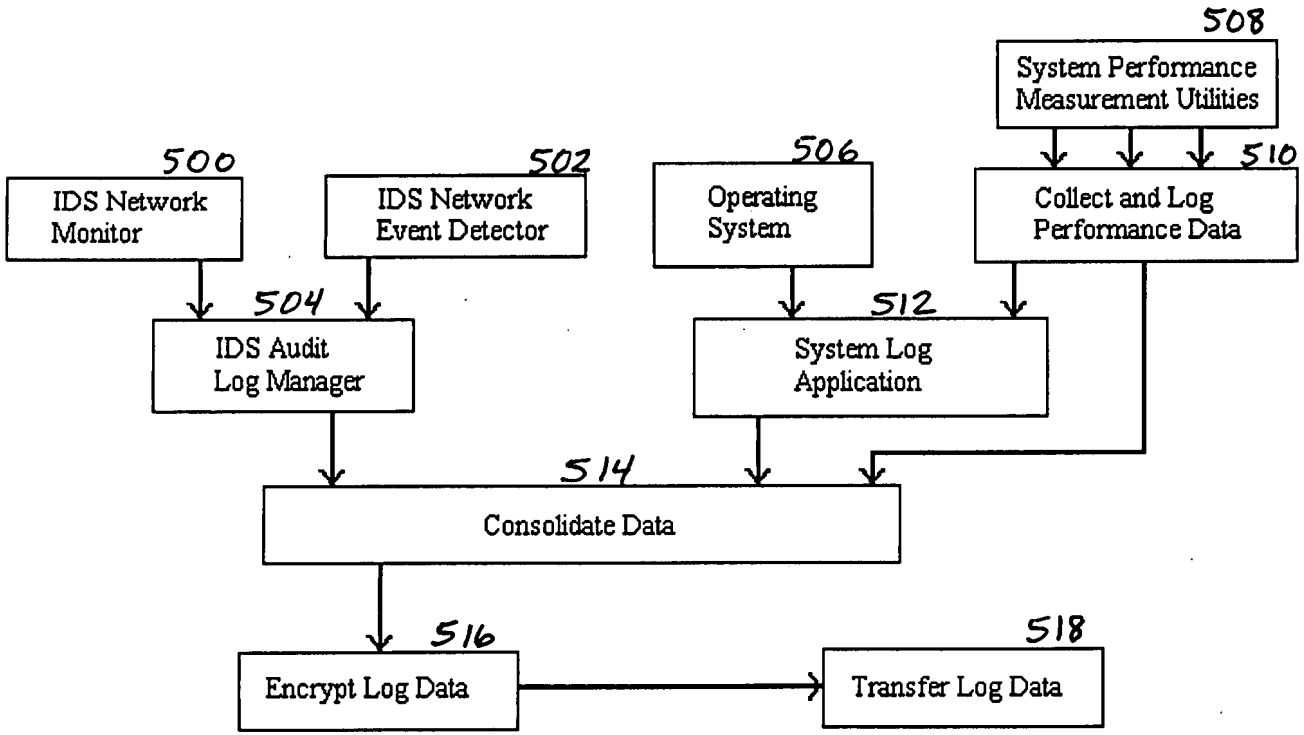

508
System Performance Measurement Utilities
500
IDS Network Monitor
502
IDS Network Event Detector
506
Operating System
510
Collect and Log Performance Data
504
IDS Audit Log Manager
512
System Log Application
514
Consolidate Data
516
Encrypt Log Data
518
Transfer Log Data

Figure 6

Transaction Table 700

xaction id	name	description		stream id	system type id	conditional
X200154	Network Transaction	A record of a network transaction through a CyberGuard firewall		R100204	T100001	($Action == "T")
X317189	CPU Utilization	A record of CPU percent idle, percent system, percent I/O, and percent user		R113203	T100001	TRUE

System Type Table 702

system type id	make	model	title	load	version	revision	patch
T100001	CyberGuard Corp	3412-02	CyberGuard Firewall For UNIX	CyberGuard	2	2.3	11

Stream Table 704

stream id	stream_type	stream path	end of record	end of field
R100204	DELIMITED_FLAT_FILE	/var/audit_logs/old/NetguardD	NEWLINE	SPACE
R113203	FIXED_FORM_FLAT_FILE	/store/compressed/stat.log	NEWLINE	N_A

Figure 7

Element Table 706

xaction id	element id	name	description	legal value	data unit	refresh period	sample period	period unit	aggregate
X200154	E312073	Date	Date of network transaction	DATE_ISO	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312074	Time	Time of network transaction	TIME_24	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312075	Action	Transaction Type	CHAR	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312076	Source_IF	Name of source firewall network interface	ALPHANUMERIC	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312077	Destination_IF	Name of destination firewall network interface	ALPHANUMERIC	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312078	Source_Address	Source IP address of packet	IP_4	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312079	Destination_Address	Destination IP address of packet	IP_4	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312080	Protocol	IP protocol of packet	IP_PROTOCOL	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312081	Source_Port	Source port number / service name of packet or ICMP type	ALPHANUMERIC	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312082	Destination_Port	Destination port number / service name of packet or ICMP type	ALPHANUMERIC	N_A	ASYNC	SYNC	N_A	N_A
X200154	E312083	Packets_Sent	Number of packets passed from source to destination	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N_A	N_A
X200154	E312084	Packets_Received	Number of packets passed from destination to source	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N_A	N_A
X200154	E312085	Bytes_Sent	Number of bytes passed from source to destination	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N_A	N_A
X200154	E312086	Bytes_Received	Number of bytes passed from destination to source	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N_A	N_A
X317189	E444120	Date	Date of measurement	DATE_ISO	N_A	1	10	MINUTE	AVERAGE
X317189	E444121	Time	Time of measurement	TIME_24	N_A	1	10	MINUTE	AVERAGE
X317189	E444122	CPU Idle	Percent CPU Idle	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444123	System Percentile	Percent of CPU used for system tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444124	I/O Percentile	Percent of CPU used for I/O tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444125	User Percentile	Percent of CPU used for user tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE

Delimited Flat File Table 708

element id	encoding	record num	field num	subfield delim	subfield num	start in field	end in field
E312073	ASCII_7_BIT	ALL	1	NONE	0	0	0
E312074	ASCII_7_BIT	ALL	2	NONE	0	0	-1
E312075	ASCII_7_BIT	ALL	3	NONE	0	0	0
E312076	ASCII_7_BIT	ALL	4	/	1	0	0
E312077	ASCII_7_BIT	ALL	4	/	2	0	0
E312078	ASCII_7_BIT	ALL	5	NONE	0	0	0
E312079	ASCII_7_BIT	ALL	6	NONE	0	0	0
E312080	ASCII_7_BIT	ALL	7	NONE	0	0	0
E312081	ASCII_7_BIT	ALL	8	NONE	0	0	0
E312082	ASCII_7_BIT	ALL	9	NONE	0	0	0
E312083	ASCII_7_BIT	ALL	10	NONE	0	0	0
E312084	ASCII_7_BIT	ALL	11	NONE	0	0	0
E312085	ASCII_7_BIT	ALL	12	NONE	0	0	0
E312086	ASCII_7_BIT	ALL	13	NONE	0	0	0

Fixed Form Flat File Table 710

element id	encoding	record num	start in record	end in record
E444120	ASCII_7_BIT	ALL	1	10
E444121	ASCII_7_BIT	ALL	12	19
E444122	ASCII_7_BIT	ALL	21	23
E444123	ASCII_7_BIT	ALL	24	26
E444124	ASCII_7_BIT	ALL	27	29
E444125	ASCII_7_BIT	ALL	30	32

Figure 8

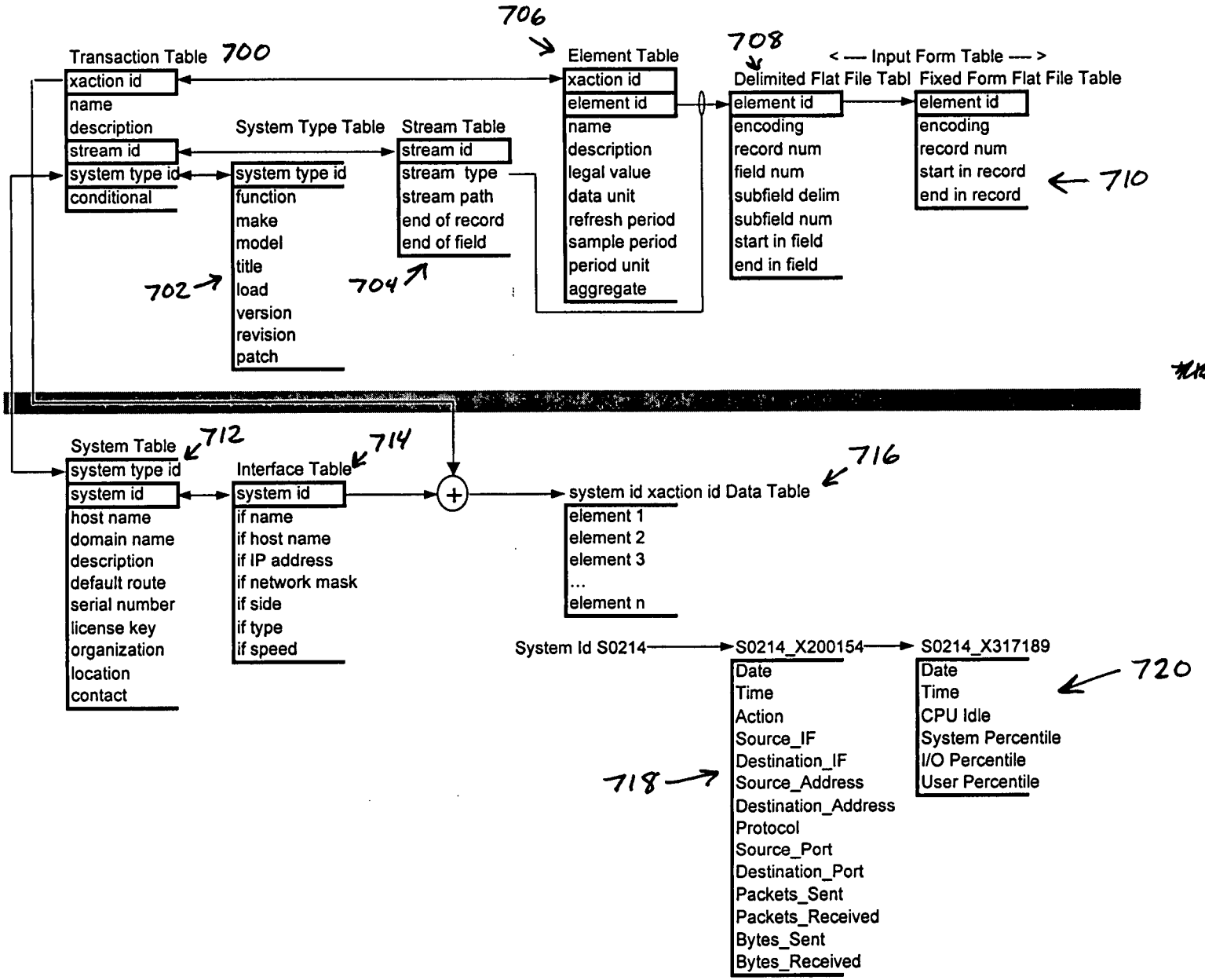

706
708
Transaction Table 700
xaction id
name
description
stream id
system type id
conditional
System Type Table
system type id
function
make
model
title
load
version
revision
patch
Stream Table
stream id
stream type
stream path
end of record
end of field
Element Table
xaction id
element id
name
description
legal value
data unit
refresh period
sample period
period unit
aggregate
< — Input Form Table — >
Delimited Flat File Tabl
element id
encoding
record num
field num
subfield delim
subfield num
start in field
end in field
Fixed Form Flat File Table
element id
encoding
record num
start in record
end in record
710
702
704
712
714
716
System Table
system type id
system id
host name
domain name
description
default route
serial number
license key
organization
location
contact
Interface Table
system id
if name
if host name
if IP address
if network mask
if side
if type
if speed
system id xaction id Data Table
element 1
element 2
element 3
...
element n
System Id S0214
S0214_X200154
Date
Time
Action
Source_IF
Destination_IF
Source_Address
Destination_Address
Protocol
Source_Port
Destination_Port
Packets_Sent
Packets_Received
Bytes_Sent
Bytes_Received
S0214_X317189
Date
Time
CPU Idle
System Percentile
I/O Percentile
User Percentile
718
720

Figure 9

1999/10/2709:00:00043004010023
1999/10/2709:10:00022003005010
1999/10/2709:20:00043004010023
1999/10/2709:30:00043004010023
1999/10/2709:40:00043004010023
1999/10/2709:50:00043004010023

Figure 10

S0214_X317189 Data Table

Date	Time	CPU Idle	System Percentile	I/O Percentile	User Percentile
1999/10/27	09:00:00	43	4	10	23
1999/10/27	09:10:00	22	3	5	10
1999/10/27	09:20:00	43	4	10	23
1999/10/27	09:30:00	43	4	10	23
1999/10/27	09:40:00	43	4	10	23
1999/10/27	09:50:00	43	4	10	23